

Method and System for Displaying Network Security Incidents

ABSTRACT OF THE INVENTION

A network security monitor system groups a plurality of security events into network sessions, correlates the network sessions according to a set of predefined network security event correlation rules and generates a security incident for the network sessions that satisfy one of the network security event correlation rules. The system then presents the information of the network sessions and security incidents to a user of the system in an intuitive form. The user is able to not only learn the details of a possible network attack, but also creates new security event correlation rules intuitively, including drop rules for dropping a particular type of events.